DIGITAL SIGNATURE SYSTEM AND METHOD BASED ON HARD LATTICE PROBLEM

ABSTRACT OF THE DISCLOSURE

A sender computer maps a randomized concatenation of a message μ to a point "x" in space using a function that renders it infeasible that a second message can be mapped nearby the message μ. The function can be a collision intractable or non-collision intractable function that maps the message to a point "x" on a widely-spaced grid, or the function can map the message to a point "x" of an auxiliary lattice. In either case, the sender computer, using a short basis (essentially, the private key) of a key lattice $\mathscr{L}$, finds a lattice point "y" that is nearby the message point "x", and then at least the points "x", "y", and message are sent to a receiver computer. To verify the signature, the receiver computer simply verifies that "y" is part of the lattice using a long basis (essentially, the public key), and that the distance between "x" and "y" is less than a predetermined distance, without being able or having to know how the lattice point "y" was obtained by the sender computer.